

Current Threat Environment

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Mark Sherman, PhD
Technical Director, CERT
mssherman@sei.cmu.edu

29-Aug-2014



Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 29 AUG 2014		2. REPORT TYPE N/A		3. DATES COVERED	
4. TITLE AND SUBTITLE Current Threat Environment				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Sherman /Mark S.				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited.					
13. SUPPLEMENTARY NOTES The original document contains color images.					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT SAR	18. NUMBER OF PAGES 16	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			



Copyright 2014 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution.

This material was prepared for the exclusive use of Participants of C3E Workshop and may not be used for any other purpose without the written consent of permission@sei.cmu.edu.

Carnegie Mellon® and CERT® are registered marks of Carnegie Mellon University.

DM-0001785





Current Threat Environment

- Usual view of threat environment
- Looking backwards from today's threats
- Looking forwards to future threats
- The need for prevention is pressing



Usual view of threat environment



Sources: Poneman Institute, CNNMoney study, May 28, 2014; McAfee Quarterly Threat Report, June 2014; Wall Street Journal, Feb 26, 2014

retailcustomerexperience.com - 5_lessons_learned_from_recent_retail_data_breaches.pdf



Looking backwards from today's threats



92% of the 100,000 incidents from the last 10 years can be described by 9 basic patterns

- Insider misuse
- DOS attacks
- Cyber-espionage
- Crimeware
- Web app attacks
- Physical theft and loss
- Payment card skimmers
- Point-of-sale intrusions
- Miscellaneous errors





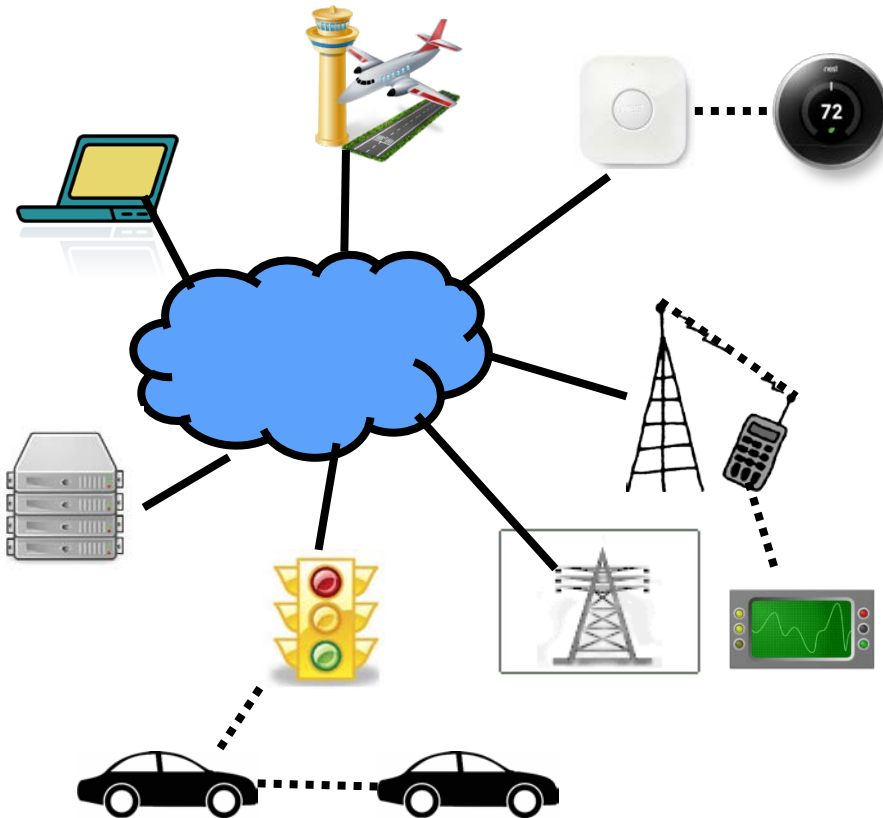
Looking forward to future threats



- Technology
- Evolving role of people in cyber security
- Learning from data: measurements, metrics, analysis



Cyber threats track evolution of technology



- Software is the new hardware
- Covering the next last mile
- Expanding endpoints





Software is the new hardware

IT moving from specialized hardware to software, virtualized as

- Memory
- Storage
- Servers
- Switches
- Networks

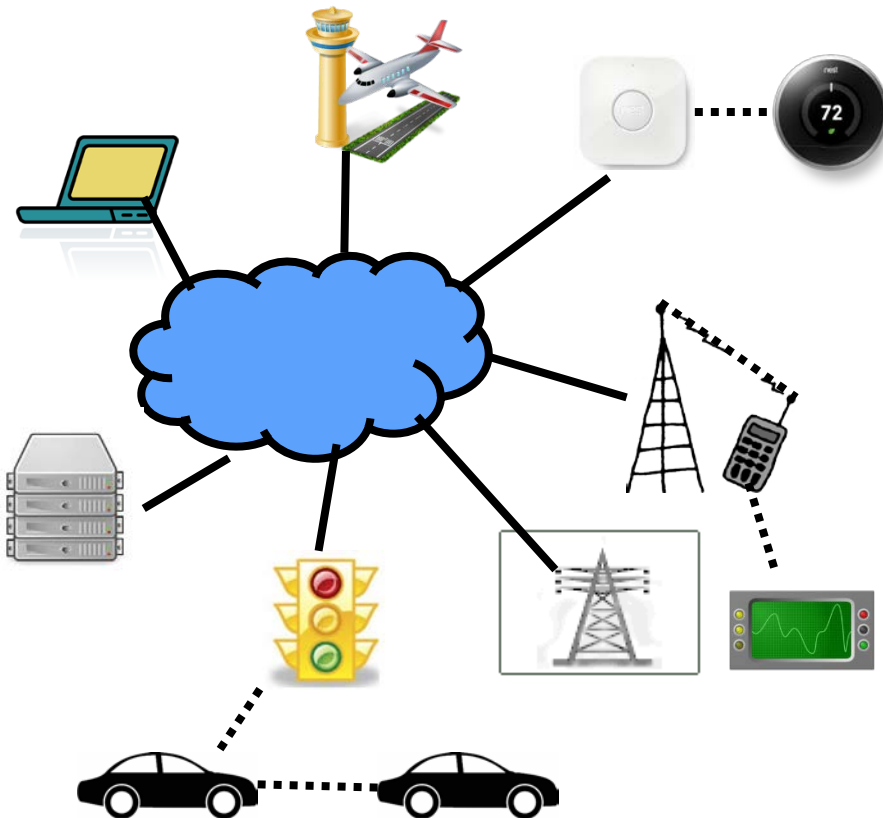
Cyber-physical systems (CPS) evolving to a computer with interesting peripherals

- Airplane function in software moved from 8% to 80% since 1960
- Software defined radios drive communication
- Television evolved to digital signal processors

- Hardware security needs software analogs
- New programming models need secure coding guidelines
- Guard against side channel attacks enabled by virtualization



Covering the next last mile – securing the border and end points



The last mile has expanded to

- Cellular
 - Main processor
 - Base band processor
 - Secure element (SIM)
- Industrial and home automation
 - SCADA
 - Bluetooth
 - Zigbee
- Automotive
 - Intravehicular: more than 50 networked processors
 - Vehicle to infrastructure (V2I): congestion management, emergency services, law enforcement
 - Vehicle to vehicle (V2): safety, efficiency
- Aviation
 - Fly by wire
 - Next Gen air traffic control
- Smart grid
- Embedded medical devices





Evolving role of people in cyber security

Analysts: Soaring need for cyber analysts

- Bureau of Labor Statistics projects information security analyst jobs to increase by 20% or more through 2018
- Need validated measurement and testing of needed skills, at individual and team level

Optimizing analyst effectiveness: Automation assists analysts

- What can be automated and what left to the analyst
- Trade off between training and application

Developers: Development becoming assembly over creation

- At least 75% of organizations rely on open source as the foundation of their applications
- Weak or absent security tracking in the software supply chain

Adversaries: Culture role in cyber security

- Cultural influences on development and attack behavior



Learning from data: measurements, metrics, analysis

$$\frac{\partial}{\partial a} \ln f_{a, \sigma^2}(\xi_1) = \frac{(\xi_1 - a)}{\sigma^2} f_{a, \sigma^2}(\xi_1) = \frac{1}{\sqrt{2\pi\sigma}} \exp\left(-\frac{(\xi_1 - a)^2}{2\sigma^2}\right)$$
$$\int_{\mathbb{R}_n} T(x) \cdot \frac{\partial}{\partial \theta} f(x, \theta) dx = M\left(T(\xi) \cdot \frac{\partial}{\partial \theta} \ln L(\xi, \theta)\right) \int_{\mathbb{R}_n} \frac{\partial}{\partial \theta} T(x) f(x, \theta) dx$$
$$\int_{\mathbb{R}_n} T(x) \cdot \left(\frac{\partial}{\partial \theta} \ln L(x, \theta)\right) \cdot f(x, \theta) dx = \int_{\mathbb{R}_n} T(x) \cdot \left(\frac{\partial}{\partial \theta} \frac{f(x, \theta)}{f(x, \theta)}\right) \cdot f(x, \theta) dx$$
$$\frac{\partial}{\partial \theta} \int_{\mathbb{R}_n} T(x) f(x, \theta) dx = \int_{\mathbb{R}_n} \frac{\partial}{\partial \theta} T(x) f(x, \theta) dx$$

Biggest challenges

- Determining leading indicators
- Reducing false positives

Need to extract information from data from across the software lifecycle

Applying techniques across disciplines including

- Metric and model definition
- Social and psychological experimentation
- Machine learning
- Statistical modeling

Applications to

- Real-time analysis
- Retrospective insight





An ounce of prevention is worth a pound of cure

“We wouldn't have to spend so much time, money, and effort on network security if we didn't have such bad software security.”

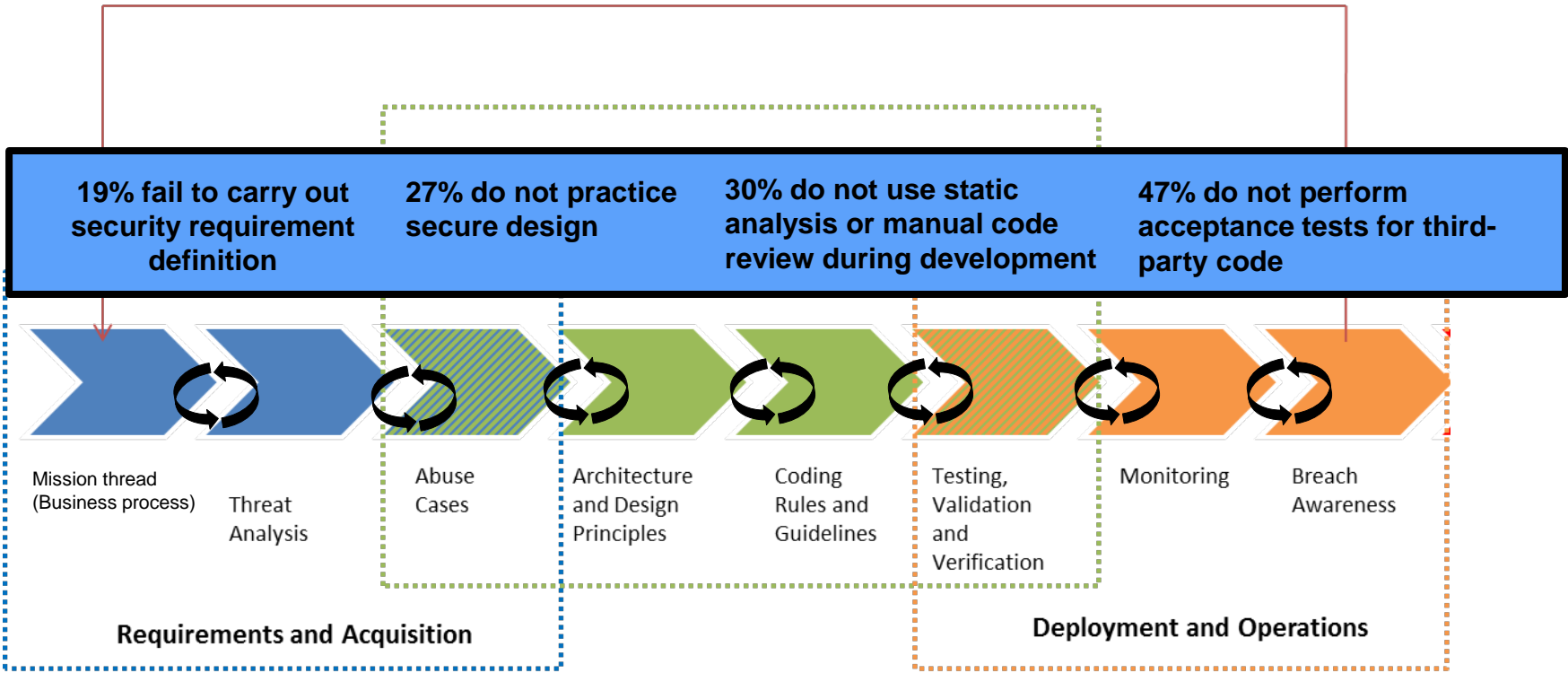
Bruce Schneier in Viega and McGraw,
“Building Secure Software,” 2001





The need for prevention is pressing

Sustainment



More than 81% do not coordinate their security practices in various stages of the development life cycle.

Source: Forrester Consulting, "State of Application Security," January 2011



Security by default





Contact Information

Mark Sherman

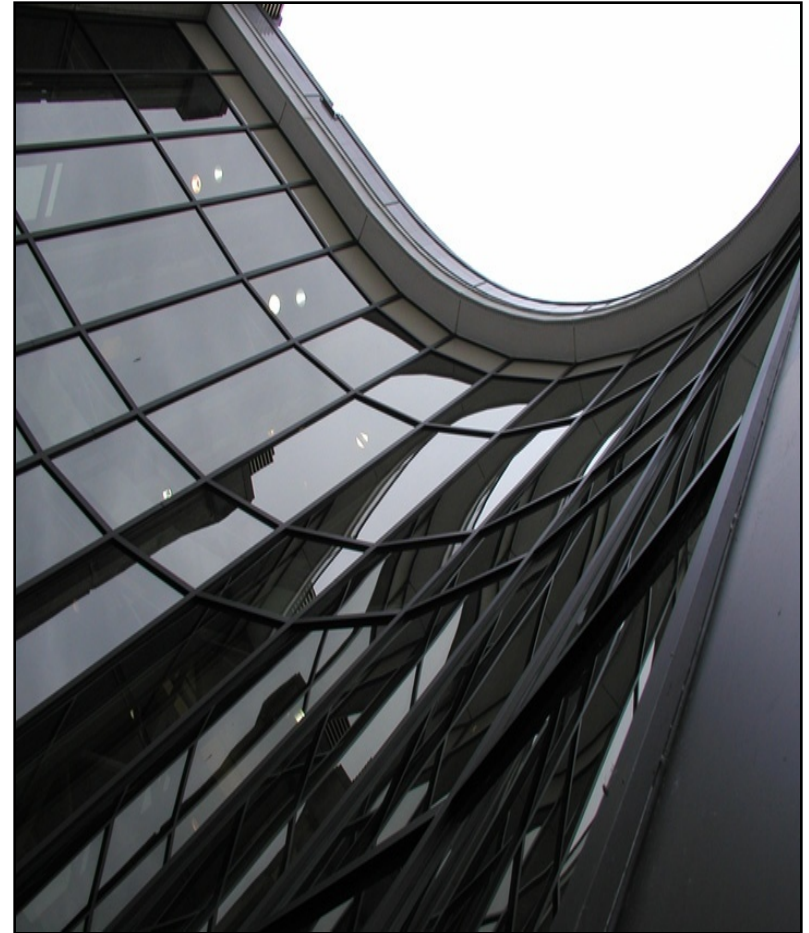
(412) 268-9223

mssherman@sei.cmu.edu

Web Resources (CERT/SEI)

<http://www.cert.org/>

<http://www.sei.cmu.edu/>



Software Engineering Institute

Carnegie Mellon University

Mark Sherman
Cyber Security Foundations Research
© 2014 Carnegie Mellon University



Software Engineering Institute

Carnegie Mellon University



Software Engineering Institute

Carnegie Mellon University

Mark Sherman
Cyber Security Foundations Research
© 2014 Carnegie Mellon University